UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,153	12/21/2001	Chui-Shan Teresa Lam	09469.010001	5605

22511 7590 05/17/2005

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
HEWITT II, CALVIN L	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/037,153	LAM ET AL.	
	Examiner	Art Unit	
	Calvin L Hewitt II	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20 and 22-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20 and 22-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Status of Claims

1. Claims 1-20 and 22-35 have been examined.

Response to Amendment/Arguments

2. Applicant has amended the claims to include the limitation of "wherein data is used to generate a key in the key management system". However, such an addition fails to distinguish Applicant's method and apparatus from the cited prior art as Auerbach et al. teach a method for generating keys from data (column 5, lines 4-8).

Regarding the 101 rejection to claims 18-20 and 22-35, Applicant asserts the claims are "useful" as they produce an encrypted serial file (Remarks, page/line 7/30-8/3). However, Applicant's "encrypted serial file" is not in the claims. Therefore, the claims continue to lack "use". The claims are also inoperable as the encryption key, after being hashed cannot be recovered.

Regarding the 112 rejection, "-tuple" is understood in the art of [mathematical] analysis (e.g. advanced calculus, functional) as a pair unless the term is preceded by an "n" or "m", where n or m is a natural number. For example, the 3-tuple (x,y,z) represents a coordinate in R^3 or 3-space.

The Examiner maintains the rejection.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 18-20 and 22-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 18 and 34 describe an algorithm. The "usefulness" of such an algorithm is not apparent, as the outcome merely results in the storage of a number or similar mathematical construct, and was produced without transformation of the data by a machine, such as a computer mathematical construct without a practical application. Hence the claimed invention does not produce useful, concrete and tangible result (*State Street Bank & Trust Co. v. Signature Financial Group Inc.,* 149 F.3d 1368, 1373, 47 USPQ2d 1596, 1600 (Fed. Cir. 1998)).

Claims 19-33 are also rejected as they depend from claim 18.

5. Claims 18-20 and 22-35 are rejected under 35 U.S.C. 101 because the claimed invention is the disclosed invention is inoperative and therefore lacks utility.

Claims 18, 34 and 35 recite the creation and storage of a hashed encryption key. Special functions such as MDx (MD2, MD4, MD5) are one-way hash functions (Specification, paragraph 26). One-way functions are "secure" in that they operate on a value to produce a "hash", however, a similar or inverse operation does not exist such that the value can be reproduced from the hash. To one of ordinary skill the hash of a file is used to verify the authenticity of the original file by calculating a second hash of the file and comparing. In the Applicant's teaching the encryption key is hashed and stored presumably for future manipulation (Specification, paragraphs 42 and 43). Therefore, as the encryption key cannot be recovered the Applicant's method and apparatus does not have any use.

Claims 19, 20, and 22-33 are also rejected as they depend from claim 18.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 18-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 18, 34 and 35 recite the creation and storage of a hashed encryption key. Special functions such as MDx (MD2, MD4, MD5) are one-way hash functions (Specification, paragraph 26). One-way functions are "secure" in that they operate on a value to produce a "hash", however, a similar or inverse operation does not exist such that the value can be reproduced from the hash. To one of ordinary skill the hash of a file is used to verify the authenticity of the original file by calculating a second hash of the file and comparing. In the Applicant's teaching the encryption key is hashed and stored presumably for future manipulation (Specification, paragraphs 42 and 43). Therefore, as the encryption key cannot be recovered it is not clear, to one of ordinary skill, what exactly the Applicant is claiming.

Claims 24 and 25 are also rejected as they refer to a "tuple"(i.e. a pair) with more than two elements.

Claims 19-33 are also rejected as they depend from claim 18.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claim 1-9 and 17 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Auerbach et al., U.S. Patent No. 5,673,316.

As per claims 1-9 and 17 Auerbach et al. teach a network system for key management comprising:

- a server (figure 1; column 2, lines 11-15)
- a key management system providing process logic for key management system initialization located on the server, secure data storage, and an interface for providing a means for inputting data into key management system (figure 1; column 2, lines 11-15; column 6, lines 50-61)
- a client computer, comprising a user interface (GUI or browser) for inputting data into the key management system, connected to the server (figure 1; column 1, lines 54-60; column 6, lines 50-61; column 8, lines 5-15; column/line 8/45-9/10)
- key management storage located on a server or on a second server connected to the server (figure 1; column 2, lines 10-15)
- connecting client and server using an encrypted connection (column 8, lines 20-25 and 58-62; column 10, lines 35-40)

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 10-16 and 18-20 and 22-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Auerbach et al., U.S. Patent No. 5,673,316.

As per claims 10 and 12-14, Auerbach et al. teach a network key management system comprising a memory for storing data with (figure 1; column 2, lines 11-15), a hashing module (using MD5) for hashing a key encrypting key and an encryption (or encoding) module, comprising key generation (column 5, lines 1-8), for encrypting data (column 5, lines 5-43; column/line 5/54-6/43; column 6, lines 15-28). Regarding serialization, Auerbach et al. teach distribution over networks such as the internet (column 1, lines 55-65). More specifically, Auerbach et al. disclose compression techniques (column 4, lines 19-25; column 5, lines 55-62). Therefore, it would have been obvious to one of ordinary skill to apply compression algorithms to the cryptographic envelope (figure 5) in order to reduce storage (column 4, lines 19-25) and thereby facilitate more efficient transmission.

As per claim 11, Auerbach et al. disclose randomizing data (column 5, lines 1-8).

As per claims 15 and 16, Auerbach et al. teach a key generation tool that comprises a symmetric algorithm (column 5, lines 1-8) and a key generation tool that comprise asymmetric algorithms, for example for encrypting and decrypting data exchanged by client and server (column 7, lines 30-42; column 8, lines 22-25 and 58-63; column 9, lines 40-48; column 10, lines 35-40).

As per claims 18-20 and 22-35, Auerbach et al. teach:

- entering data and a key encryption key into a key management system (abstract)
- combining data into a tuple (e.g. document part and control part) (figure 2)
- encrypting the tuple (encoding a key field of the tuple) with the key encryption key to create a token (abstract; figure 2)
- hashing the encryption key (figure 3)
- storing the token in a vector (column/line 3/58-4/2)
- storing the hashed key (figures 2 and 3)
- storing a list of keys (figures 2 and 3)
- randomizing data (column 5, lines 1-8)
- randomizing the list of keys and secret tokes (figure 3)
- generating data to encrypt (abstract; figure 2)

- a tuple with an application, key, value and type field (figure 3)
- key management storage located on a server or on a second server connected to the server (figure 1; column 2, lines 10-15)
- a client computer, comprising a user interface (GUI or browser) for inputting data into the key management system, connected to the server (figure 1; column 1, lines 54-60; column 6, lines 50-61; column 8, lines 5-15; column/line 8/45-9/10)

Regarding serialization (-the flattening of an N-dimensional object in to a one-dimensional object or "vector"), Auerbach et al. teach distribution over networks such as the internet (column 1, lines 55-65) (note as the n-dimensional object is the cryptographic envelope). More specifically, Auerbach et al. disclose compression techniques (column 4, lines 19-25; column 5, lines 55-62). Therefore, it would have been obvious to one of ordinary skill to apply compression algorithms to the cryptographic envelope (figure 5) in order to reduce storage (column 4, lines 19-25) and thereby facilitate more efficient transmission. Regarding "tagging" the method and system of Auerbach et al. is implemented using computer code (column/line 3/59-4/8). More specifically, Auerbach et al. teach cryptographic envelopes as executables, subroutines, modules or object components hence in order to be manipulated objects have to be defined (i.e. tag). Regarding algorithms, teach a key generation tool that

comprises a symmetric algorithm (column 5, lines 1-8) and a key generation tool that comprise asymmetric algorithms, for example for encrypting and decrypting data exchanged by client and server (column 7, lines 30-42; column 8, lines 22-25 and 58-63; column 9, lines 40-48; column 10, lines 35-40).

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone

number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (571) 272-6712.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

c/o Technology Center 2100

Washington, D.C. 20231

or faxed to:

(703) 305-7687 (for formal communications intended for entry and after-final communications),

or:

(571) 273-6709 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Calvin Loyd Hewitt II

May 3, 2005

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600